UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

AOD FEDERAL CREDIT UNION, on behalf of itself and all others similarly situated, Plaintiff, v. THE WENDY'S COMPANY, WENDY'S RESTAURANTS, LLC, and WENDY'S INTERNATIONAL, LLC, Defendants.	Case No. _____ CLASS ACTION COMPLAINT Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff AOD Federal Credit Union, on behalf of itself and all others similarly situated, alleges the following against Defendants The Wendy's Company, Wendy's Restaurants, LLC, and Wendy's International, LLC (collectively, "Wendy's" or "Defendants"), based upon on personal knowledge where applicable, information and belief, and the investigation of counsel.

I. INTRODUCTION

1. Despite the well-publicized and ever growing threat of cyber breaches involving payment card networks and systems, Wendy's systematically failed to ensure that it maintained adequate data security measures and failed to comply with industry standards by allowing its computer and point of sale systems to be hacked causing financial institution's payment card and customer information to be stolen.

2. In January 2016, news first surfaced that Wendy's was investigating a breach of its computer systems. According to a security alert received by VISA, the period at which credit card data was exposed was from October 22, 2015 through March 10, 2016. However, Wendy's

later admitted that the breach has yet to be contained. VISA has stated that the data that was exposed by the data breach included Track 1 and Track 2 data which normally includes the accountholder's name, primary account number (PAN), expiration date, service code, and verification code. Beginning at a time unknown to Plaintiff, a group of hackers took advantage of substantial weaknesses and vulnerabilities in Wendy's computer and point of sale systems by installing malware to extract payment card data from customer's credit and debit cards. Using the malware they installed, the hackers were able to steal Wendy's customers' payment card information and other payment card data ("PCD"), as well as personal identifiable information ("PII") that Wendy's had collected in conjunction with customers' restaurant purchases (collectively, "Customer Data").

3. The data breach was the inevitable result of Wendy's inadequate data security measures and approach to data security. Wendy's data security deficiencies were so significant that hackers were able to install malware and remain undetected for months, until outside parties notified Wendy's that its computer and point of sale systems may have been breached as a result of the identification of fraudulent transactions that had taken place after the hackers had used or sold the Customer Data.

4. On May 11, 2016, Wendy's issued a press release on Form 8-K with the United States Securities and Exchange Commission.[1] In this press release, Wendy's acknowledged that several hundred of its restaurants were impacted by "malware" that was "installed through the use of compromised third-party vendor credentials," and which "affected one particular point of sale system." Despite evidence to the contrary, Wendy's May 11th announcement assured consumers and banks that the breach impacted just five percent of stores.

[1] https://www.sec.gov/Archives/edgar/data/30697/000119312516586362/d158377dex991.htm.

5. On June 9, 2016, however, approximately four and a half months after news of the data breach first broke, Wendy's admitted that the number of stores impacted was "significantly higher" and that the intrusion may not yet be contained. Even then, Wendy's refused to be more specific about what restaurants were involved

6. The financial costs caused by Wendy's deficient data security approach have been borne primarily by the financial institutions, like Plaintiff, that issued the payment cards compromised in the data breach. These costs include, but are not limited to, canceling and reissuing compromised cards and reimbursing their customers for fraudulent charges. Industry sources estimate that the fraudulent charges have been more pervasive than in other recent data breaches (*e.g.*, Target and Home Depot), causing Plaintiff and other members of the Class to suffer much greater losses.

7. This class action is brought on behalf of financial institutions throughout the United States to recover the damages that they and others similarly situated have suffered as a direct result of the Wendy's data breach. Plaintiff asserts claims for negligence, negligence *per se*, and declaratory and injunctive relief.

II. PARTIES

8. Plaintiff AOD Federal Credit Union is a federally chartered credit union with its principal place of business located in Oxford, Alabama. As a result of the Wendy's data breach, Plaintiff has suffered injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

9. Defendant The Wendy's Company is a Delaware corporation with its principal place of business in Dublin, Ohio.

10. Defendant Wendy's Restaurants, LLC is a Delaware limited liability company whose sole member is The Wendy's Company.

11. Defendant Wendy's International, LLC is an Ohio limited liability company whose parent company is Wendy's Restaurants, LLC.

12. Wendy's is engaged in the business of operating, developing and franchising a system of quick-service restaurants. According to Wendy's Form 10-K filed with the Securities and Exchange Commission for the year ending January 3, 2016, Wendy's restaurant system was comprised of 6,479 restaurants, of which 632 were owned and operated by Wendy's. In 2015, its revenues totaled approximately $1.9 billion.

III. JURISDICTION AND VENUE

13. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from one defendant, there are more than 100 Class members, and the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs. This Court has personal jurisdiction over Wendy's because it conducts substantial business in this district.

14. The Western District of Pennsylvania has personal jurisdiction over Defendants named in this action because Defendants conduct substantial business in this District.

15. Venue is proper in this district under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in this district and Defendants have caused harm to Class members residing in this district.

IV. FACTUAL ALLEGATIONS

16. It is well known that Customer Data is valuable and often targeted by hackers. Over the last several years, numerous data breaches have occurred at large retailers and

restaurants nationwide, including Home Depot, Target, KMART, P.F. Chang's, and many others. Despite the increasing occurrences of data breaches of systems of other restaurants and retailers, Wendy's refused to take steps to adequately protect its computer systems from intrusion.

17. In early January, financial institutions and Wendy's customers around the country began incurring unauthorized charges on payment card accounts. One customer noted that she suspected that her credit card information was stolen in early January after visiting a Wendy's in Illinois.

18. In late January, news sources reported that a breach had likely occurred after some banks noticed a pattern of fraud on cards that had all recently been used at Wendy's restaurants.[2] Wendy's said that it had already begun receiving reports earlier in January. Wendy's, instead of acknowledging the breach and alerting all financial institutions out of caution, stated that "it's not appropriate just yet to speculate on anything in terms of scope." On January 27, 2016, Wendy's announced that it was investigating reports of "unusual activity" on payment cards used in some of its restaurants, but refused to acknowledge that a data breach had occurred, reiterating that "it is difficult to determine with certainty the nature or scope of the potential incident."[3]

19. It was not until February 9, 2016, nearly two weeks after the public reports surfaced, that Wendy's acknowledged publicly that "some [of its locations] have been found by the cybersecurity experts to have malware on their systems." Attempting to downplay the seriousness of the breach, Wendy's assured customers that financial institutions—like Plaintiff

---

[2] *Wendy's Probes Reports of Credit Card Breach*, KREBS ON SECURITY (Jan 27, 2016), http://krebsonsecurity.com/2016/01/wendys-probes-reports-of-credit-card-breach/ (last visited Mar. 28, 2016).

[3] http://www.wsj.com/articles/wendys-investigating-reports-of-unusual-activity-on-payment-cards-used-at-some-restaurants-1453911780.

and other members of the class—would reimburse Wendy's customers for any fraudulent charges.

20. Wendy's made a similar, statement in its March 3, 2016 Annual Report on Form 10-K filed with the United States Securities and Exchange Commission, stating that "the Company has engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity related to certain Wendy's restaurants. Out of the locations investigated to date, some have been found by the cybersecurity experts to have malware on their systems. The investigation is ongoing, and the Company is continuing to work closely with cybersecurity experts and law enforcement officials."

21. On May 11, 2016, Wendy's filed a press release on Form 8-K with the United States Securities and Exchange Commission. In this press release, Wendy's acknowledged that several hundred of its restaurants were impacted from "malware" that was "installed through the use of compromised third-party vendor credentials," and which "affected one particular point of sale system." Despite evidence to the contrary, Wendy's May 11th announcement assured consumers and banks that the breach impacted just five percent of stores.

22. VISA, one of the payment card networks, issued a VISA Compromised Account Management System or "CAMS" alert, that was sent to at least some financial institutions by VISA, indicating that the estimated "exposure window" for the Wendy's data breach runs from October 26, 2015 through March 10, 2016. On June 9, 2016, however, approximately four and a half months after news of the data breach first broke, Wendy's admitted that the number of stores impacted was "significantly higher" and that the intrusion may not yet be contained.

23. This means that Wendy's failed to prevent or stop the hackers from stealing Customer Data for approximately six months.

24. The CAMS alert further indicates that both Track 1 and Track 2 data may have been compromised in the data breach. Track 1 and Track 2 data normally include credit and debit card information such as cardholder name, primary account number, expiration date, and in certain instances PIN number.

25. Taking advantage of Wendy's lax data security and delayed notification to financial institutions and the public, hackers were able to gather large amounts of Customer Data. With that data, unknown perpetrators were able to make hundreds of thousands or even millions of fraudulent undetected purchases on credit and debit cards that had been issued by Plaintiff and members of the Class. Unknown perpetrators also specifically targeted and drained debit accounts with large amounts of money in them, concentrating the damages and causing individual financial institutions, such as Plaintiff and members of the Class, significant losses. Indeed, given the duration of the Wendy's data breach—approximately six months—hackers appeared to have had near unfettered access to Wendy's computer and point of sale systems to obtain significant Customer Data. At first, Wendy's failed to acknowledge that its systems had been subjected to a breach. Yet even after acknowledging the breach in late January 2016, it still took Wendy's several more months to stop it. These failures demonstrate the shortcomings of Wendy's data security systems, as well as Wendy's woefully inadequate response to the breach.

26. Wendy's knew that a breach of its point of sale systems was possible and could cause serious disruption to its business. Specifically, in its Form 10-K filed with the Securities and Exchange Commission for the year ending January 3, 2016, Wendy's listed as one of its potential risk factors, a data breach involving financial information from its POS systems:

> ***We are heavily dependent on computer systems and information technology and any material failure, interruption or security breach of our computer systems or technology could impair our ability to efficiently operate our business.***

> Any security breach involving our or our franchisees' point-of-sale or other systems could result in a loss of consumer confidence and potential costs associated with fraud. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur, resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. A security breach of our computer systems or information technology could require us to notify customers, employees or other groups, result in adverse publicity, loss of sales and profits, and incur penalties or other costs that could adversely affect the operation of our business and results of operations.

Wendy's Jan. 3, 2016 Form 10-K at 20.

27. Despite acknowledging such risks, Wendy's disregarded the potential danger of a data breach by negligently failing to take adequate steps to prevent and stop hackers from gaining access to Wendy's computer systems.

28. Wendy's also failed to prevent or mitigate damages by refusing to promptly disclose to financial institutions and the public the fact that a data breach had occurred.

A. Wendy's POS Systems Were Outdated

29. In 2012, Wendy's announced plans to implement a new POS platform for the entire Wendy's system in the U.S. and in Canada. Wendy's admitted in connection with a lawsuit against a franchisor that Wendy's existing POS systems were outdated and that a system wide POS upgrade was necessary. Compl. at 9, *Wendy's Int'l, LLC v. DavCo Rests., LLC*, No. 14-cv-013382 (Ct. Comm. Pls., Franklin Cty. Ohio) (attached as Exhibit A). However, Wendy's franchisee, DavCo Restuarants LLC, in its counterclaim alleged that the new POS system was fraught with serious technical and operational problems and that Wendy's has acknowledged such problems and called them unreasonable. DavCo Counterclaim at 10 (attached as Exhibit B). DavCo further alleged that Wendy's has issued an indefinite suspension of most installations

of the new POS system. DavCo Counterclaim at 11. Specifically, DavCo alleges that Wendy's had previously rejected the POS system it was recommending its franchisees install. DavCo Counterclaim at 15. Moreover, the allegations further state that the POS software at issue has stability issues, repeatedly froze and disconnected from the store's network. DavCo Counterclaim at 15-16.

B. Wendy's Failed to Follow Card Operating Regulations

30. Payment card processors and networks, including VISA and MasterCard, issue Card Operating Regulations that are binding on Wendy's. Such regulations were in place long before the data breach.

31. The Card Operating Regulations required Wendy's to protect cardholder data and prevent its unauthorized disclosure; prohibited Wendy's from storing such data, even in encrypted form, longer than necessary to process the transaction; and mandated compliance with industry standards.

32. Wendy's violated the Card Operating Regulations because it failed to maintain adequate data security measures to protect the security and confidentiality of its customers' payment card information, inappropriately stored cardholder data, and as explained in more detail below, violated industry standards.

C. Wendy's Failed to Upgrade its Payment Systems to Utilize EMV Technology

33. The payment card industry also set rules requiring all businesses to upgrade to new card readers that accept EMV chips. EMV chip technology uses imbedded computer chips instead of magnetic stripes to store payment card data. Unlike magnetic-stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used again. Such

technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the thieves making it much more difficult for criminals to profit from what is stolen.

34. The payment card industry (MasterCard, VISA, Discover, and American Express) set a deadline of October 1, 2015 for businesses to transition their systems from magnetic-stripe to EMV technology. Wendy's did not meet that deadline.

35. Under Card Operating Regulations, businesses accepting payment cards but not meeting the October 1, 2015 deadline agree to be liable for damages resulting from any data breaches.

36. Despite the availability of this superior, more secure technology, Wendy's refused its implementation. Gavin Waugh, vice president and treasurer at Wendy's, stated, "I don't think that would have solved this problem."

D. Wendy's Failed to Comply with Industry Standards

37. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Data Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of payment card data, although it sets the minimum level of what must be done, not the maximum.

38. PCI DSS 3.1, the version of the standards in effect at the time of the data breach, imposed the following twelve "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS 3.1, furthermore, set forth detailed and comprehensive requirements that had to be followed to meet each of the twelve mandates.

39. Among other things, PCI DSS required Wendy's to properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data to those with a need to know; establish a process to identify and timely fix security vulnerabilities; assign unique identification numbers to each individual with access to its systems; and encrypt payment card data at the point of sale.

E. Wendy's Failed to Comply with FTC Requirements

40. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

41. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's

vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

42. The FTC also has published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

43. The FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

44. In the years leading up to the Wendy's data breach and during the course of the breach itself, Wendy's failed to follow the guidelines recommended by the FTC. Furthermore, by failing to have reasonable data security measures in place, Wendy's engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

F. Wendy's Failed to Comply with Other Legal Requirements

45. Several states have enacted data breach statutes that require merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code § 1798.81.5(b) and Wash. Rev. Code § 19.255, or that otherwise impose data security obligations on merchants, such as Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64. States have also adopted unfair and deceptive trade practices acts, which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. Moreover, most states have enacted statutes requiring merchants to provide notice if their

data security systems are breached. These statutes, implicitly or explicitly, support the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

46. Wendy's failed to have reasonable security protections like those outlined above in place at the time of the instant data breach and failed to provide timely notice of the breach. As a result, Wendy's violated the terms of these types of state statutes.

G. The Data Breach Damaged Financial Institutions

47. The data breach caused substantial damage to Plaintiff and class members, who had to act immediately to mitigate the massive fraudulent transactions being made on payment cards that they had issued, while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but Plaintiff and class members are not. Financial institutions bear primary responsibility for reimbursing customers for fraudulent charges on the payment cards they issue.

48. As a result of the Wendy's data breach, Plaintiff and class members have been forced to cancel and reissue payment cards, change or close accounts, notify customers that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage. Furthermore, debit and credit cards belonging to class members and Plaintiff—as well as the account numbers on the face of the cards—were devalued. Such damage is ongoing, as Wendy's has yet to contain the breach.

49. The financial damages suffered by Plaintiff and members of the class are significant and are ongoing. Industry sources estimate that millions of accounts could be affected by the data breach.

50. According to B. Dan Berger, Chief Executive Officer of the National Association of Federal Credit Unions, before Wendy's had even acknowledged the data breach, one credit CEO reported:

> Please take this Wendy's story very seriously. We have been getting killed lately with debit card fraud. We have already hit half of our normal yearly fraud so far this year, and it is not even the end of January yet. After reading this, we reviewed activity on some of our accounts which had fraud on them. The first six we checked had all been to Wendy's in the last quarter of 2015.
>
> All I am suggesting is that we are experiencing much high[er] losses lately than we ever did after the Target or Home Depot problems. I think we may end up with 5 to 10 times the loss on this breach . . . .[4]

H. Plaintiff's Facts

51. Plaintiff AOD Federal Credit Union issued VISA-branded payment cards (debit and credit) to its members.

52. By at November 2015, Plaintiff had begun to notice an increase in fraudulent transactions on its members' payment cards, many of which had been used to make purchases at Wendy's restaurants.

53. On April 26, 2016, Plaintiff received a CAMS alert from VISA indicating that cards issued by Plaintiff were compromised in a suspected breach at Wendy's.

54. As a result of the Data Breach, Plaintiff incurred significant costs associated with, among other things, notifying customers/members of issues related to the Data Breach, closing

[4] http://krebsonsecurity.com/2016/03/credit-unions-feeling-pinch-in-wendys-breach/.

out and opening new customer/member accounts, reissuing customers'/members' cards, refunding customers'/members' losses resulting from the unauthorized use of their accounts, costs to investigate fraudulent charges, and/or costs due to lost interest and transaction fees due to reduced card usage. Plaintiff was forced to reissue approximately 2,241 payment cards to its customers at a cost of approximately $5.00 per card. Such damage is ongoing, as Wendy's has yet to contain the breach.

V. CLASS ACTION ALLEGATIONS

55. Plaintiff brings this action on behalf of itself and as a class action pursuant to the provisions of Rules 23(a) and 23(b)(3) of the Federal Rules of Civil Procedures on behalf of the following class (the "Class"):

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases from Wendy's while malware was installed on its payment card systems.

56. Excluded from the Class are Defendants and their subsidiaries and affiliates; all employees of Defendants; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned and his/her immediate family and his/her court staff.

57. Certification of Plaintiff's claims for class-wide treatment is appropriate because all elements of Fed. R. Civ. P. 23(a) and 23(b)(3) are satisfied. Plaintiff can prove the elements of its claims on a class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

58. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all

Class members is impracticable. While Plaintiff is informed and believes that there are thousands of members of the Class, the precise number of Class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

59. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. Whether Defendants engaged in the misconduct alleged herein;

b. Whether Wendy's owed a duty to Plaintiff and members of the class to protect cardholder personal and financial data;

c. Whether Wendy's failed to provide adequate security to protect consumer cardholder personal and financial data;

d. Whether Wendy's negligently or otherwise improperly allowed cardholder personal and financial data to be accessed by third parties;

e. Whether Wendy's failed to adequately notify Plaintiff and members of the class that its data systems were breached;

f. Whether Wendy's failed to adequately and, in a timely manner, contain or otherwise prevent hackers' access to customer data;

g. Whether Plaintiff and members of the class were injured and suffered damages and ascertainable losses;

h. Whether Wendy's failure to provide adequate security proximately caused Plaintiff's and class members' injuries;

i. Whether Plaintiff and members of the class are entitled to damages and, if so, the measure of such damages; and

j. Whether Plaintiff and members of the class are entitled to declaratory and injunctive relief.

60. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class, having issued payment cards that were compromised in the Wendy's data breach. Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendants' conduct.

61. **Adequacy of Representation:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because it is a member of the Class and its interests do not conflict with the interests of the other members of the Class that it seeks to represent. Plaintiff is committed to pursuing this matter for the Class with the Class' collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type, and Plaintiff intends to prosecute this action vigorously. Plaintiff and its counsel will fairly and adequately protect the Class's interests.

62. **Predominance and Superiority:** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's individual case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment

suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I
Negligence

63. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

64. Wendy's owed—and continues to owe—a duty to Plaintiff and the Class to use reasonable care in safeguarding Customer Data and to notify them of any breach in a timely manner so that compromised financial accounts and credit cards can be closed quickly in order to avoid fraudulent transactions. This duty arises from several sources, including but not limited to the sources described below, and is independent of any duty Wendy's owed as a result of its contractual obligations.

65. Wendy's has a common law duty to prevent the foreseeable risk of harm to others, including Plaintiff and the Class. That injury that would result from Wendy's failure to use reasonable measures to protect Customer Data and to provide timely notice of a breach was foreseeable. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Customer Data belonging to millions of Wendy's customers; thieves would use

Customer Data to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud such as by cancelling and reissuing the compromised cards and reimbursing their customers for fraud losses; and that the resulting financial losses would be immense.

66. Wendy's assumed the duty to use reasonable security measures as a result of its conduct.

67. A duty to use reasonable security measures arose as a result of the special relationship that existed between Wendy's and the financial institutions—Plaintiff and members of the Class. The special relationship arose because financial institutions entrusted Wendy's with Customer Data from payment cards they issued. Only Wendy's was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

68. Wendy's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Customer Data by businesses such as Wendy's. The FTC publications and data security breach orders described above further from the basis of Wendy's duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty.

69. Wendy's duty to use reasonable care in protecting Customer Data arose not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards regulations, specifically including PCI DSS.

70. Wendy's breached its common law, statutory and other duties, and thus was negligent, by failing to use reasonable measures to protect its customers' personal and financial information from the hackers who perpetrated the data breach and by failing to provide timely notice of the breach. Upon information and belief, the specific negligent acts and omissions committed by Wendy's include, but are not limited to, some or all of the following:

a. failure to delete cardholder information after the time period necessary to authorize the transaction;

b. failure to employ systems to protect against malware;

c. failure to regularly update its antivirus software;

d. failure to maintain an adequate firewall

e. failure to track and monitor access to its network and cardholder data;

f. failure to limit access to those with a valid purpose;

g. failure to encrypt PII at the point-of-sale;

h. failure to transition to the use of EMV technology;

i. failure to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;

j. failure to assign a unique ID to each individual with access to its systems;

k. failure to automate the assessment of technical controls and security configuration standards;

l. failure to adequately staff and fund its data security operation;

m. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations;

n. failure to recognize red flags signaling that Wendy's systems were inadequate and that as a result the potential for a massive data breach was increasingly likely;

o. failure to recognize that hackers were stealing Customer Data from its network while the data breach was taking place;

p. failure to contain the data breach or otherwise revoke hackers' access in a timely manner;

q. failure to disclose the data breach in a timely manner.

71. In connection with the conduct described above, Wendy's acted wantonly, recklessly, and with complete disregard for the consequences.

72. The individuals at Wendy's who committed the negligent acts and omissions include Wendy's officers and directors and others who are not named.

73. As a direct and proximate result of Wendy's negligence, Plaintiff and members of the Class have suffered and continue to suffer injury, including but not limited to, cancelling and reissuing payment cards, changing or closing accounts notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage resulting from the beach, and the cards they issued (and the corresponding account numbers) were rendered worthless. Such damage is ongoing, as Wendy's has yet to contain the breach.

COUNT II
Negligence *Per Se*

74. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

75. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses such as Wendy's of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described above also form the basis of Wendy's duty.

76. Wendy's violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards, including PCI DSS as described in detail herein. Wendy's conduct was particularly unreasonable given the nature and amount of Customer Data it obtained and stored and the foreseeable consequences of a data breach at an international restaurant, including specifically the immense damages that would result to consumers and financial institutions.

77. Wendy's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

78. Plaintiff and members of the Class are within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, many of the Class members are credit unions, which are organized as cooperatives whose members are consumers.

79. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable

data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

80. As a direct and proximate result of Wendy's negligence *per se*, Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless. Such damage is ongoing, as Wendy's has yet to contain the breach.

COUNT III
Declaratory and Injunctive Relief

81. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

82. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

83. An actual controversy has arisen in the wake of Wendy's data breach regarding its common law and other duties to reasonably safeguard Customer Data. Plaintiff alleges that Wendy's data security measures were inadequate and remain inadequate. Wendy's denies these allegations. Furthermore, Plaintiff continues to suffer injury as additional fraudulent charges are being made on payment cards they issued to Wendy's customers.

84. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Wendy's owed and continues to owe a legal duty to secure its customers' personal and financial information—specifically including information pertaining to credit and debits cards used by Wendy's customers—and to notify financial institutions of a data breach under the common law, Section 5 of the FTC Act, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

b. Wendy's breached, and continues to breach, this legal duty by failing to employ reasonable measure to secure its customers' personal and financial information;

c. Wendy's breach of its legal duty proximately caused the data breach; and

d. Banks, credit unions, and other institutions that reissued payment cards and were forced to pay for fraudulent transactions as a result of the Wendy's data breach are legally entitled to recover the costs they incurred from Wendy's.

85. The Court also should issue corresponding injunctive relief requiring Wendy's to employ adequate security protocols consistent with industry standards to protect its customers' personal and financial information. Specifically, this injunction should, among other things, direct Wendy's to:

a. contain the breach or otherwise revoke hackers' access to Wendy's data networks;

b. utilize industry standard encryption to encrypt transmission of cardholder data at the point-of-sale and at all other times;

c. implement encryption keys in accordance with industry standards;

d. implement EMV technology;

e. consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;

f. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

g. regularly test its systems for security vulnerabilities, consistent with industry standards;

h. comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information; and

i. install all upgrades recommended by manufacturers of security software and firewalls used by Wendy's.

86. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Wendy's if an injunction is issued. Among other things, if another massive data breach occurs at Wendy's, Plaintiff and the members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Wendy's of complying with an injunction by employing reasonable data security measures is relatively minimal, and Wendy's has a pre-existing legal obligation to employ such measures.

87. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at

Wendy's, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court:

A. Certify the Class and appoint Plaintiff and Plaintiff's counsel to represent the Class;

B. Enter a money judgment in favor of Plaintiff and members of the Class to compensate them for the injuries suffered together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

C. Enter a declaratory judgment in favor of Plaintiff and the Class as described above;

D. Grant Plaintiff the injunctive relief requested;

E. Award Plaintiff and the Class reasonable attorneys' fees and costs of suit;

F. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable.

Dated: June 20, 2016

Respectfully submitted,

CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP

/s/ Gary F. Lynch

Gary F. Lynch, PA #56887
Jamisen A. Etzel, PA #311554
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243

Fax: (412) 231-0246
Email: glynch@carlsonlynch.com
Email: jetzel@carlsonlynch.com

Brian C. Gudmundson
Jason R. Lee
ZIMMERMAN REED, LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Tel: (612) 341-0400
Fax: (612) 341-0844
brian.gudmundson@zimmreed.com
jason.lee@zimmreed.com

Jonathan L. Kudulis
TRIMMIER, KUDULIS, REISINGER, LLC
2737 Highland Avenue South
Birmingham, AL 35205
Tel: (205) 251-3151
Fax: (205) 322-6444
jkudulis@trimmier.com

Chris T. Hellums
Jonathan S. Mann
PITTMAN, DUTTON & HELLUMS, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
Fax: (205) 328-2711
chrish@pittmandutton.com
jonm@pittmandutton.com

Attorneys for Plaintiff and the Proposed Class